Smart Grid Interoperability Panel (SGIP)
Cyber Security Working Group (CSWG)
Standards Review

CSWG Standards Review Report on

Security Assessment of SAE J2847-1: Communication between Plug-in Vehicles and the Utility Grid

November 12, 2010

Security Assessment of SAE J2847-1: Communication between Plug-in Vehicles and the Utility Grid

1. Introduction

1.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different "layers" in the communications "stack" or "profile." One example of such a profile is the Grid Wise Architecture Council (GWAC)[1] Stack. Some standards address the lower layers of the communications stack, such as wireless media, fiber optic cables, and power line carrier. Others address the "transport" layers for getting messages from one location to another. Still others cover the "application" layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Since they are abstract, cybersecurity technologies cannot be linked to them until they are translated into "bits and bytes" by mapping them to one of the semantic structures. Above the communications standards are other security standards that address business processes and the policies of the organization and regulatory authorities.

Secondly, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. Cybersecurity must address those aspects outside of the communications system in the upper GWAC stack layers that may just be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to: cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Thirdly, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself: how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC stack may address issues of data importance.

Fourthly, some standards do not mandate their provisions using "shall" statements, but rather use statements such as "should," "may," or "could." Some standards also define their provisions as being "normative" or "informative." Normative provisions often are expressed with "shall" statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the "shall," "should," "may," and/or "could" statements, "normative," or "informative" language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or "profile" of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of policy, procedural, and communication standards designed to provide specific services. Ultimately,

[1]GridWise Architecture Council, http://www.gridwiseac.org/pdfs/interopframework_v1.pdf

cybersecurity as applied to the information exchange standards should be described as profiles of technologies and procedures which can include both "power system" methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if TCP/IP is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then TLS (transport layer security) should most likely (but not absolutely) be used. For some specific Smart Grid communication standards, such as International Electrotechnical Commission (IEC) 61850 and IEC 60870-6, specific cybersecurity standards (IEC 62351 series) were developed to meet typical implementations of these standards.

In the following discussions of information exchange standard(s) being reviewed, these caveats should be taken into account.

1.2 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as "appropriate security technologies and procedures should be implemented."

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

1.3 References and Terminology

References to the National Institute of Standards and Technology (NIST) security requirements refer to the NIST Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, Chapter 3, High-Level Security Requirements.

References to "Government-approved cryptography" refer to the list of approved cryptography suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees[2]:

[2] The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after "which") comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

- Requirements are expressed by "…shall…," which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).
- Recommendations are expressed by "…should…," which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).
- Permitted or allowed items are expressed by "…may…," which is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).
- Ability to carry out an action is expressed by "…can …," which is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).
- The use of the word *must* is deprecated, and should not be used in these standards to define mandatory requirements. The word *must* is only used to describe unavoidable situations (e.g. "All traffic in this lane must turn right at the next intersection.")

2. SAE J2847-1: Communication between Plug-in Vehicles and the Utility Grid

2.1 Description of Standard

The Recommended Practice, SAE J2847-1: Communication between Plug-in Vehicles and the Utility Grid "*establishes requirements and specification between plug-in electric vehicles and the electric power grid, for energy transfer and other applications.*" It addresses "*the technologies of electric vehicles, the grid, and information processing, including: (1) support for bi-directional energy transfer between vehicle and grid (FPF and RPF, as defined above); (2) support for new local communications media between vehicle and EVSE (to replace SAE J1850), such as power line communication (PLC) and wireless transports (Zigbee, WiFi, etc.); (3) synchronizing with a major revision of SAE J1772TM which includes new connectors and signals between the vehicle and EVSE, and additional AC and DC power levels; (4) support for new vehicle architectures such as plug-in hybrid (PHEV) and plug-in fuel cell (PFCV) vehicles; (5) support for new rechargeable energy storage system (RESS) technologies and packaging methods; (6) support for vehicle telematic communication transports; and (7) support for new developments in both utility and customer premises equipment, such as advanced metering infrastructure (AMI) and home-area network (HAN) technologies.*"[3]

SAE J2847-1, referencing the Use Cases of SAE J2836-1, *Use Cases for Communication Between Plug-in Vehicles and the Utility Grid*, defines the information in messages and the protocols to be used in the GWAC stack Network Interoperability layer, as well as other aspects of information exchanges between the Plug-In Vehicle and the utility whose grid it is connected to. This covers 1) the information that could or should be included in different types of messages, and 2) a discussion of the different layers of the Open Systems Interconnection (OSI) stack. The primary contents of this document are the information elements to be included in exchanges between different actors.

The standard is organized as follows:

1. Sections 1-3 includes scope, references, and definitions
2. Section 4.1: *System Definition*, references the Use Cases in SAE J2836
3. Section 4.2: *Equipment and Devices*, provides some general information, including one brief security section on the security requirements for the lower layers of the OSI stack.

[3] SAE J2847-1: Communication between Plug-in Vehicles and the Utility Grid, *Scope* and *Rationale*

4. Section 4.3: *Messages*, defines the information elements to be included in messages in tabular form along with some descriptions of the meaning or implication of the information elements.
5. Section 4.4: *Communication Layers*, describes the layers of the OSI stack to be used, with the assumption that they will be based on the Smart Energy Profile version 2 (SEP 2.0), which has not yet been developed. No other protocol stacks are identified, even though SEP 2.0 is not expected to be used for utility information exchanges.
6. Section 5: *Notes*, describes the change bars used in updates.
7. Appendix A: *Example Message Flows* provides examples.

2.2 Assumptions and Issues

The document contains a mixture of "shall" and "should" so that the normative versus informative requirements are unclear, particularly since the document is a recommended practice, not a standard. This makes security assessments difficult.

There is no description of the architecture or potential configurations, making assessments of security requirements for different interfaces very difficult.

Some statements in the document are not correct (e.g. stating that power line carrier is the preferred medium between the PEV and the utility). Assessing the security aspects of these types of statements are therefore difficult.

The document is also a mixture of GWAC-stack layers, ranging from listing the data to be exchanged (semantic), the messages (syntactic), the network (network), and media (basic connectivity). Since the architecture is not defined, assessing the security requirements for this mixture of layers is difficult.

It is not expected in the power industry that SEP 2.0 will be used for communications with the utility systems that would be exchanging many of the messages, but that protocol is the only one discussed. SEP 2.0 is not yet developed, so that assessing its security capabilities is not possible at this time.

2.3 Summary of Cybersecurity Content

2.3.1 Does the standard address cybersecurity? If not, should it?

Section *4.2.1.3 Security,* partially addresses security for the GWAC-stack Network Interoperability layer of the GWAC stack, calling for the use of IETF RFCs such as Entity Authentication Protocol (EAP) RFC 3748 for the link layer. Additional protocol support can be provided through use of Protocol for Carrying Authentication for Network Access (PANA) Framework (RFC 5191). These protocols are to be used for presentation of credentials and authentication of PEV devices joining a network. Application layer security is provided through Transport Layer Security (TLS), RFC 5246. It also calls for RFC 4492 (elliptical curve with TLS) which has not been finalized by the IETF and should not be deployed. Section 4.4.4, *Layer 4 Transport*, also references the use of TLS (RFC 5246).

2.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?

SAE J2847-1 only addresses cybersecurity for the GWAC-stack Network Interoperability layer of a single protocol suite. It does not address the security for other protocol suites, nor for higher layer requirements. It also does not address privacy issues.

The cybersecurity for these information exchanges at other layers of the GWAC-stack should be addressed in this standard or through a reference to another standard.

The correlations between this document and the security requirements described in NISTIR 7628, *Guidelines to Smart Grid Cybersecurity*, Chapter 3, families and requirements, are shown in Table 1:

Table 1: Correlations between Standard being Assessed and the NISTIR Security Requirements

Reference in Standard[4]	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
4.2.1.3 Security and 4.4.4 Layer 4 Transport	SG.SC-8 Communication Integrity	Only applicable at the GWAC-stack Network Interoperability layer. Neither the Syntactic Interoperability layer nor the Semantic Understanding layer is addressed
	SG.SC-12 Use of Validated Cryptography	Listed some cryptographic suites that are in the NIST FIPS approved list, but did not reference the NIST FIPS approved list itself.
4.4.1 Layer 1 Physical	SG.AC-16 Wireless Access Restrictions	

2.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

In Section 4.2.1.3, *Security,* the terminology used does not clearly convey what the standard requires. The terms "is," "may," and "shall," are used interchangeably.

The following families of National Institute of Standards and Technology (NIST) Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, high-level security requirements are not addressed and should be addressed at some level in this or a referenced document. Additional more specific issues are also noted:

- Access control (SG.AC) (e.g. passwords, least privilege, role-based access control);
- Auditing and accountability (SG.AU);
- Security assessment (SG.CA);
- Continuity of operations (SG.CP) is addressed functionally (e.g. on loss of communications) but not for security (e.g. security breach);
- Identification and Authentication (SG.IA) is addressed in that devices have IDs, but is not addressed with respect to security (authentication);
- Incident Response (SG.IR) is not addressed even from a functional level;
- Media Protection (SG.MP) is not addressed except functionally that PLC is more likely to be secure than wireless media;
- Information System and Services Acquisition (SG.SA) is not addressed, including supply chain protection;
- System and Communication Protection (SG.SC) is not addressed above the Network Layer, nor is key management at the Network Layer; and

[4] The references may be just the section numbers or could include the title of the section

- If PLC, wireless, or other potentially radiating technology is used for the communications, the traffic between the PEV and the EVSE should be encrypted. If no encryption, shielding, or other electromagnetic protection methods are used, there is a potential that confidential information (e.g., vehicle ID, credit card numbers, etc.) may be radiated in the clear between the EVSE and the PEV over power line carrier or wireless media.
- Section 4.3.3.2 refers to a customer PIN being entered through a "NAV" which is otherwise undefined. If the NAV is inside the car, encryption may be required for exchange with the EVSE.
- There are some decisions that need to be made regarding the use of TLS and are unaddressed. For example, these include what to do if a certificate expires.
- There may be some further information that needs to be specified about the use of EXI. Some of that information involves defining the MIME types if EXI is used with XML Encryption so the decoder will properly interpret the message.
- Since this is Recommended Practice, the word “shall” should not be used for any items that are just being recommended, not mandated.
- Any security Use Cases that will be added should be reflected in this document (or if security is deleted from this document, as recommended, addressed in the appropriate security document).
- There is absolutely no mention of a privacy policy governing anything in this standard. There is no mention of giving customer notice of information being collected and stored. Neither is there any consent requested or choice given as to what is being collected. The data to be collected is defined, but what that data is being used for is fairly open–ended.
- Within the messages being exchanged from the EUMD or PEV to the utility are data items that specifically identify the PEV (VIN) and the individual customer (Account Number, other?). Also exchanged may be information on charging location as well as some undefined, for the most part, user preferences. General privacy issues result from a lack of definition on what data is being collected and stored, lack of specifics on how customer specific data will be limited/protected, and a number of instances in which it says the utility may want to collect data for statistical or other purposes.
- In Section 4.3.3 – The subsection on Identification Messaging outlays the collection of data that will uniquely identify a PEV and/or a customer. One suggestion for the customer ID is the account number the utility has on file for the customer. There are no other suggestions given, or limitations on what should not be used (SSN, for instance). A suggestion for the vehicle ID is the VIN. Some may have privacy concerns over the use of a VIN.
- In Section 4.3.6 – The Subsection on Timing Information messaging notes that charging information specific to each customer may be collected and used for other purposes. To the extent that there are privacy implications with the possible release of this data, this standard does not limit, or otherwise define how the data being gathered can be used.

- In Section 4.3.6.3 – Here it is left to the equipment manufacturer to determine what historical data is retained to assist customers in explaining potential deviations in pricing. While I cannot foresee a privacy concern with the storage of requests for pricing data, data retention risks and recommendations should be referenced. It is not clear to me why the utility or the customer should not be in charge of the settings that control collection of historical data, as opposed to the OEM.
- In Section 4.3.7.2 – This notes that, while it is not necessary to collect and gather SOC information, the utility may want to do it for other purposes, specifically compiling usage

statistics or grid management purposes. One of the principles recommended by the privacy group is to collect only the information necessary to provision service. If this information is not necessary for such purpose, should it be collected? If so, should there be some notice to the customer that such information is being collected for purposes other than providing service to that customer. Further, if data is going to be gathered, that means retention and perhaps there should be some discussion of retention standards, or that utilities should follow applicable retention standards (not that the U.S. has any).

- The underlying architectural assumptions may have cybersecurity concerns, such as privacy violations and/or identity theft possibilities if EVSEs are compromised.

In general, this document does not include security for the GWAC-stack Syntactic Interoperability layer nor the Semantic Understanding layer, even though information exchange requirements at those layers are described in the SAE document. The discussions of security at the Network Interoperability layer are inadequate and inappropriate for the focus of this document.

Given these serious deficiencies in addressing cybersecurity, the CSWG recommends the following:

- ***Remove all references to cybersecurity and develop a separate, corresponding cybersecurity document.*** *Because there are many missing cybersecurity requirements,* ***it is recommended that Section 4.3.1.2 and all references to cybersecurity be removed from this document*** *and that another document or documents be developed to address cybersecurity for these information exchanges.*

- ***Remove the mapping to SEP2.0 in order to separate semantic standards from their mappings to different protocols that will have different cybersecurity technologies.*** *Because the SEP 2.0 protocol is not yet defined, may not be used by utility operational systems, and because other protocols could be used to support the messages defined in Section 4.3 in different architectures with different cybersecurity technologies,* ***it is recommended that Section 4.4 be removed*** *- in other words, keep the semantic standards separate from the various protocols which could transport those messages.*

- ***Ensure consistency with the results of other PAPs****. Role of the Internet Protocol Suite (IPS) in the Smart Grid, developed as an output of PAP 01,*[5] *does not include EAP (RFC 3748), but instead identifies EAP-TLS (RFC 5216), which in turn references EAP (RFC 3748). Consistency between PAP 1 and PAP 11 would be a good goal, but is not absolutely required.*

- ***Reference the FIPS-approved list of cryptography suites.*** *The acceptable cyber cryptography suites are listed, which may limit future applicability. It is suggested that the document reference the Federal Information Processing Standard (FIPS)-approved list of cryptography suites.*

- ***References to unfinalized IETF RFCs should be removed****. The reference to IETF RFC 4492 should be removed until the IETF finalizes the RFC.*

The CSWG strongly recommends that this document be removed from the results of PAP 11 and taken up by the next V2G PAP and/or DEWG for completion in order to ensure that cybersecurity is adequately addressed. Once the document is removed from the set of PAP 11 results, the CSWG expects to approve the remaining PAP 11 documents.

[5] SGIP PAP 1: *Internet Protocols for the Smart Grid*: draft-baker-ietf-core-09

2.3.4 What work, if any, is being done currently or planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

No known activity at this time, although it is expected that either a new PAP or DEWG will be formed to address any issues that remain unresolved.

2.3.5 List any references to other standards and whether they are normative or informative.

2.3.5.1 Normative Standards

- IEC 61986 UML CIM Users Group Unified Modeling Language (UML) Model

2.3.5.2 Informative Standards and Documents

- SAE J2836/1™ Use Cases for Communication Between Plug-in Vehicles and the Utility Grid
- IEC 61968-1 Application integration at electric utilities – System interfaces for distribution management - Part 1: Interface architecture and general requirements
- IEC 61968-2 Application integration at electric utilities – System interfaces for distribution management - Part 2: Glossary
- IEC 61968-3 Application integration at electric utilities – System interfaces for distribution management - Part 3: Interface for network operations
- IEC 61968-4 Application integration at electric utilities – System interfaces for distribution management - Part 4: Interfaces for records and asset management
- IEC 61968-9 Application integration at electric utilities – System interfaces for distribution management - Part 9: Interfaces for meter reading and control
- IEC 61968-13 Application integration at electric utilities – System interfaces for distribution management - Part 13: CIM RDF Model exchange format for distribution
- IEEE 802.1AR IEEE P802.1AR/D2.2: Draft Standard for Local and Metropolitan Area Networks: Secure Device Identity http://employees.org/%7Eczmax/802.1AR/802-1ar-d2-2.pdf
- RFC 768 User Datagram Protocol http://tools.ietf.org/html/rfc768
- RFC 792 Internet Control Message Protocol http://tools.ietf.org/html/rfc792
- RFC 793 Transmission Control Protocol http://tools.ietf.org/html/rfc793
- RFC 1042] A Standard for the Transmission of IP Datagrams over IEEE 802 Networks http://tools.ietf.org/html/rfc1042
- RFC 1208 A Glossary of Networking Terms http://tools.ietf.org/html/rfc1208
- RFC 2080 RIPng for IPv6 http://tools.ietf.org/html/rfc2080
- RFC 2409 The Internet Key Exchange (IKE) http://tools.ietf.org/html/rfc2409
- RFC 2119 Key words for use in RFCs to Indicate Requirement Levels http://tools.ietf.org/html/rfc2119
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification http://tools.ietf.org/html/rfc2460
- RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing http://tools.ietf.org/html/rfc2545
- RFC 2616 Hypertext Transfer Protocol -- HTTP/1.1 http://tools.ietf.org/html/rfc2616

- RFC 2631 Diffie Hellman Key Agreement Method http://tools.ietf.org/html/rfc2631
- RFC 3117 IETF RFC 3117, On the Design of Application Protocols http://tools.ietf.org/html/rfc3117
- RFC 3748 Extensible Authentication Protocol (EAP) http://tools.ietf.org/html/rfc3748
- RFC 3766 IETF RFC 3766, Determining Strengths for Public Keys Used for Exchanging Symmetric Keys http://tools.ietf.org/html/rfc3766
- RFC 4279 Pre-Shared Key Ciphersuites for Transport Layer Security http://tools.ietf.org/html/rfc4279
- RFC 4291 IP Version 6 Addressing Architecture http://tools.ietf.org/html/rfc4291
- RFC 4302 IP Authentication Header http://tools.ietf.org/html/rfc4302
- RFC 4303 IP Encapsulating Security Payload (ESP) http://tools.ietf.org/html/rfc4303
- RFC 4306 Internet Key Exchange (IKEv2) Protocol http://tools.ietf.org/html/rfc4306
- RFC 4347 Datagram Transport Layer Security http://tools.ietf.org/html/rfc4347
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification http://tools.ietf.org/html/rfc4443
- RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security http://tools.ietf.org/html/rfc4492
- RFC 4862 IPv6 Stateless Address Autoconfiguration http://tools.ietf.org/html/rfc4862
- RFC 4919 IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals http://tools.ietf.org/html/rfc4919
- RFC 4944 Transmission of IPv6 Packets over IEEE 802.15.4 Networks http://tools.ietf.org/html/rfc4944
- RFC 5191 Protocol for Carrying Authentication for Network Access (PANA) Framework http:/tools.ietf.org/html/rfc5193
- RFC 5216 The EAP-TLS Authentication Protocol http://tools.ietf.org/html/rfc5216
- RFC 5238 Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP) http://tools.ietf.org/html/rfc5238
- RFC 5246 The Transport Layer Security (TLS) Protocol v1.2 (http://tools.ietf.org/html/rfc5246
- RFC 5247 Extensible Authentication Protocol (EAP) Key Management Framework http://tools.ietf.org/html/rfc5247
- RFC 5288 AES Galois Counter Mode (GCM) Cipher Suites for TLS http://tools.ietf.org/html/rfc5288
- RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM) http://tools.ietf.org/html/rfc5289
- RFC 5340 OSPF for IPv6 http://tools.ietf.org/html/rfc5340
- EXI Efficient XML Interchange (EXI) Format 1.0 http://www.w3.org/TR/2008/WD-exi-20080919
- REST Representational State Transfer http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm